U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

September 9, 2016

Via cybercommission@nist.gov

Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Subject: Information on Current and Future States of Cybersecurity in the Digital Economy

Dear Ms. Grayson:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, welcomes the opportunity to respond to the Commission on Enhancing National Cybersecurity's (the Commission's) request for information (RFI) about current and future states of cybersecurity in the digital economy, which the National Institute of Standards and Technology (NIST) is supporting.[1]

The Commission asks that organizations respond to approximately a dozen questions based on topics in the February 2016 executive order (EO) and the meetings that the Commission has held to date.[2] The Chamber does not attempt to answer every question in the RFI. We focus on the top three cybersecurity issues that the Chamber wants the Commission and the next administration to prioritize. We believe that it is crucial for the 45th president to get the big issues positioned correctly, so that relatively smaller issues (e.g., cyber insurance)[3] fall into place more easily.[4]

Since April, the Commission has examined numerous topics in a thoughtful and methodical way. Taken as a whole, the Chamber believes that the Commission's recommendations to the next administration do not need to solve every complex cybersecurity challenge—there are too many. Instead, the Commission should seek to (1) maintain the momentum of quality initiatives, particularly the joint industry-NIST *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework) and the new information-sharing law. The Commission should also (2) examine ways to boost adherence to international norms and deterrence.[5] The Chamber recognizes that imposing costs on malicious actors is complicated. Policymaking will require engaging the business community, making trade-offs, and allowing time for thinking to mature.

EXECUTIVE SUMMARY

Leadership on the Commission on Enhancing National Cybersecurity (the Commission) has described the report that it will present to the White House in December as a transition memo to the 45th president, which is a workable approach. The U.S. Chamber urges the Commission to prioritize the following three policy initiatives, which will help strengthen cybersecurity in the public and private sectors and enhance U.S. economic and national security.

1. **The Cybersecurity Framework: Preserving Flexibility and Collaboration, Driving International Alignment**

- *Challenge.* Businesses need a cost-effective tool that is rooted in a common language to manage their cybersecurity risks. The solution must be based on business needs without placing additional regulatory requirements on industry. Also, cybersecurity efforts are optimal when they reflect industry-driven practices and global standards.

- *Solution:* The Commission should recommend to the next administration that its No. 1 cybersecurity priority is embracing the joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework). The Framework, which the Chamber actively promotes, has received much praise from public and private organizations at home and overseas.

- *Timeline:* Right away. The private sector should eventually govern the Framework, but NIST needs to maintain a key role in collaborating with industry and engaging foreign organizations and governments.

2. **The Cybersecurity Information Sharing Act of 2015 (CISA): Building Capacity and Fostering Trust**

- *Challenge:* Most policy and business observers agree that effective cybersecurity information sharing is an important method of protecting organizations' networks and information systems. To be meaningfully actionable, threat data need to be shared in real time, which is a work in progress.

- *Solution:* President Obama signed the Cybersecurity Information Sharing Act of 2015 (CISA) into law in December 2015, which the Chamber applauds. The new law is meant to spur protected, automated sharing. CISA is off to a good start. The Chamber urges lawmakers and the 45th president to be industry's ally as it uses the program and builds capacity. Companies need to trust that policymakers have their backs.

- *Timeline:* Right away. The next administration should partner with the Chamber in urging businesses to use the Framework, join an information-sharing body, and take advantage of the CISA/Automated Information System (AIS) as appropriate. Such actions will take several years to implement.

3. **Norms and Deterrence: Negotiating Toward Acceptable Behaviors and Imposing Costs on Malicious Actors**

- *Challenge:* Despite the existence of written blueprints, the U.S. cybersecurity strategy is seemingly uncertain—both to many in the private sector and our adversaries alike—in part because of the complexity.

- *Solution:* Public-private policymaking needs to spotlight increasing adherence to international norms and deterrence (roughly equivalent to improving U.S. defenses and imposing costs on bad actors). A key goal is to reduce the benefits of conducting harmful cyber activity against the business community and the nation. The upcoming administration should engage the private sector and other stakeholders on the roles of cyber defense and deterrence. The pros and cons of cyber deterrence deserve more careful scrutiny than they have received to date.

- *Timeline:* The next administration will need to bolster norms and deterrence over its next one to two terms. The 45th president should build on the work of the Obama administration.

The remainder of this paper expands on these topics in more detail and includes additional background information.

1. THE CYBERSECURITY FRAMEWORK: PRESERVING FLEXIBILITY AND COLLABORATION, DRIVING INTERNATIONAL ALIGNMENT

The Chamber believes that businesses and policymakers see the joint industry-NIST Framework as a pillar for managing enterprise cybersecurity risks and threats, including at home and increasingly abroad.[6] NIST did an admirable job convening many organizations to develop the Framework over the course of many months. Support for the Framework has been evident throughout the Commission's four open workshops from May to August.[7]

The Chamber will press President Obama's successor to embrace the Framework. We see the Framework as a multistakeholder tool, a collaborative process, and a constructive mind-set. The Chamber urges private organizations—from the C-suite to the newest hire—to commit to robust cybersecurity practices and regular improvements.

Public-Private Collaboration

To sustain the momentum behind the Framework, the Chamber believes that both industry and government have jobs to do. On the one hand, the Chamber has been actively promoting the Framework since it was released in 2014. The Chamber launched our cybersecurity roundtable series in 2014. This national initiative recommends that businesses of all sizes and sectors adopt fundamental internet security practices, including using the Framework and similar risk management tools, engaging cybersecurity providers, and partnering with law enforcement before cyber incidents occur.

The Chamber has spearheaded 11 major regional roundtables and two summits in Washington, D.C., since 2014. More events are planned for 2017. The Chamber's *Fifth Annual Cybersecurity Summit* will be held on September 27. Each regional event includes approximately 200 attendees and typically features cybersecurity principals from the White House, DHS, NIST, and local FBI and Secret Service officials. Further, Chamber members are using the Framework and urging business partners to manage cybersecurity risks to their data and devices. Industry is working with government entities to strengthen its information networks and systems against a dizzying array of malicious actors.

On the other hand, the Chamber urges policymakers to help agencies and departments harmonize existing regulations with the Framework and maintain the Framework's flexible, nonregulatory nature. For example, in April, the Chamber engaged in a quality discussion with the Cybersecurity Forum for Independent and Executive Branch Regulators (the Cyber Forum). We indicated that some government entities are forming genuine partnerships with industry to enhance the security and resilience of U.S. critical infrastructure; some agencies are seemingly exploring ways to flex their regulatory muscles; and some federal bodies are apparently abandoning the spirit, if not the precepts, of the 2013 EO (13636) on strengthening critical infrastructure and the Cybersecurity Enhancement Act of 2014. Both measures call for identifying and reducing the cyber regulatory burden on the business community.

A single business organization should not be beset by multiple cybersecurity rules coming from many agencies, which are likely to be conflicting or duplicative in execution.

Regulation is likely to drain businesses' optional cybersecurity resources toward compliance. The Chamber holds that policymakers, including members of the Cyber Forum, should appoint an official(s) to focus on reducing duplicative, if not eliminating, overly burdensome cyber-security requirements impacting regulated organizations, as called for under the 2013 EO and the 2014 act.

It is instructive that during the August 23 Commission meeting in Minneapolis a federal agency official, when asked during a Q&A, was unable to come up with an example of how the government is attempting to harmonize government cybersecurity mandates. The official said, "I cannot come up with an example of harmonization." To be fair, even if his statement was not 100% accurate (i.e., some modicum of harmonization is happening), it is still mostly true in the Chamber's experience. We, too, cannot point to concerted efforts by government leaders to streamline existing cybersecurity regulations.

Some sectors may have multiple requirements that need to be rationalized with the Framework, while others may face less of a burden. The bottom line is that the Chamber believes that the next administration should make it a priority in 2017 to meet with sector-specific groups (e.g., associations, coordinating councils) and companies to exchange perspectives on how voluntary partnerships and regulatory programs can be made more effective for both government and industry.

In addition to urging regulatory harmonization, it is equally crucial that the next presidency opposes the creation of new or quasi-cybersecurity regulations, especially when government authorities have not taken affected entities' perspectives into account. A case in point is the Federal Communication Commission's (the FCC's or the Commission's) proposed broadband privacy rule. The Chamber believes that the FCC needs to dramatically pull back on this rulemaking. Above all, the FCC's rulemaking represents what not to do from a standpoint of collaboration. The Commission takes the opposite approach to shared, cooperative public-private cybersecurity that the Obama administration and the Chamber are holding up as a model for stakeholders to imitate.[8]

International Alignment

In addition to domestic considerations surrounding the Framework, many Chamber members operate globally. Much of U.S. industry is advocating that foreign governments and regions like the European Union (EU) align their cybersecurity programs with the Framework. The Chamber appreciates that NIST has been actively meeting with foreign governments urging them to embrace the Framework. However, NIST should not have to shoulder the outreach load alone.

The Commission should recommend that the next administration organizes opportunities for stakeholders to participate in multinational discussions. The Chamber urges the federal government to work with international partners and believes that these discussions should be stakeholder driven and occurring on a routine basis. The very nonregulatory, cooperative, and efficient qualities that have drawn industries toward the Framework—which can be used regardless of where their operations are situated internationally—attach to companies regardless of whether they are American, British, French, German, Korean, or Italian, among others.

The Framework is special because it is biased toward a standards- and technology-neutral approach to managing cybersecurity risks, rather than favoring a particular nation's or a region's processes. Virtually all multinational organizations benefit when policymakers align flexible cybersecurity risk management programs at the international level, not just at the national level. The 45th president is strongly urged to embrace the Framework. Still, the Framework is only part of a mix of cybersecurity policy initiatives, particularly implementing the new information-sharing law, which should move forward together.

2. THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (CISA): BUILDING CAPACITY AND FOSTERING TRUST

The Chamber applauds Congress and President Obama for passing the Cybersecurity Information Sharing Act of 2015 (CISA), which is title I of the Cybersecurity Act of 2015, in December 2015.[9] The Chamber led the Protecting America's Cyber Networks Coalition (the Coalition), a partnership of more than 50 leading business associations representing nearly every sector of the U.S. economy. It took a dedicated team working with Capitol Hill and the administration to get CISA done.

CISA establishes a voluntary information-sharing program intended to strengthen businesses' protection and resilience against cyberattacks. The law gives businesses legal certainty that they have safe harbor against frivolous lawsuits when freely sharing and receiving cyber threat indicators (CTIs) and defensive measures (DMs) in real time and taking actions to mitigate cyberattacks. CISA also offers protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among public and private entities.

The law safeguards individuals' privacy and civil liberties and establishes appropriate roles for government agencies and departments. CISA reflects sound compromises among many parties on these issues.[10]

CISA called for the Department of Homeland Security (DHS) to establish a "capability and process" (aka a portal) in the department to receive CTIs and DMs shared by businesses with the federal government in an electronic format—i.e., through email or media, an interactive form on an internet website, or a real-time and automated process. In March 2016, DHS launched an Automated Indicator Sharing (AIS) platform that enables the government and the private sector to exchange cybersecurity threat information with one another.[11]

On June 9, an industry participant at a DHS-led CISA implementation workshop captured the thinking of many when he said, "Our adversaries are employing automated techniques against us. Machine-to-machine sharing is a key element needed to help solve our cybersecurity problems." He added that the United States cannot succeed if we pit cyber professionals—which are a significantly limited workforce asset—against machines.

The AIS initiative reportedly has more than 100 participants—spanning the banking, energy, and technology sectors, as well as both small and large companies—up from

6 participants this past spring. Groups have begun testing their ability to share and receive indicators, but there is not yet sharing on a massive scale.[12]

The Chamber is championing CISA as part of our national cybersecurity campaign. Appropriate, real-time automated sharing will strengthen the security and resilience of industry and government, thus heightening the costs of executing malicious attacks by U.S. adversaries. Many experts contend that the timely sharing of cyber indicators among various information-sharing and analysis organizations (ISAOs), information-sharing and analysis centers (ISACs), and private- and public-sector entities can reduce both the probability and the severity of cybersecurity incidents. ISACs are considered to be ISAOs.

The enactment of CISA triggered several government guidelines and procedures. In particular, DHS and the Department of Justice (DOJ) released final guidance on June 15 to assist "non-federal entities"—including organizations in the private sector and state and local governments—to share CTIs with the federal government. The departments also released final procedures relating to the receipt and use of CTIs by the federal government, final guidelines relating to privacy and civil liberties in connection with the exchange of these indicators, and guidance to federal agencies on sharing information in the government's possession.

The Chamber's main message to the Commission concerning CISA/AIS implementation is threefold:

- The CISA program is off to a good start. We said to lawmakers in June that while oversight by Congress is crucial, it is too soon to make changes to the legislation. CISA does not need to be reauthorized for several years (i.e., September 2025).

- We urge lawmakers and the next administration to be industry's ally as it uses the program. Companies need to trust that policymakers have their backs. It is important that businesses see that the protections granted by the law—including matters tied to limited liability, regulation, antitrust, and public disclosure—become real.

  The Chamber agrees with a witness who spoke on June 21 before the Commission at the University of California-Berkeley. He noted that the government could make it easier for companies to create a "regulatory safe space," where they can more effectively share information about bugs and attacks.[13] The Chamber hears such sentiments frequently and believes that government entities like DHS want to use company data prudently. However, many more agencies and departments will have to adopt attitudes and actions that do not create disincentives to businesses reporting threat and vulnerability data. Time will tell.

- We tell businesses that they should use the Framework, join an ISAO or an ISAC, and take advantage of the CISA/AIS system as appropriate. The Chamber is pressing senior leaders of industry groups to promote these initiatives among their peers and constituencies.[14]

Private Organizations and Information-Sharing Capabilities: Different Strokes for Different Folks

The Chamber believes that businesses' use of the Cybersecurity Information Sharing Act of 2015 (CISA)/ Automated Indicator Sharing (AIS) program falls into roughly four categories. These groupings are generalizations—shorthand for where private entities are in the information-sharing ecosystem. It is important to note that policymakers need to have patience regarding industry's use of CISA and AIS.

First, not all private organizations will have the financial means and personnel to establish an information-sharing program, join information-sharing and analysis organizations (ISAOs) or information-sharing and analysis centers (ISACs), and/or plug into the AIS system—and many do not need to.

Second, the perceived success of CISA should not be dependent on the number of organizations that join AIS directly. Such a number is expected to be relatively small, according to government and industry experts. Most businesses will swap threat data among their peers and across sectors, not necessarily with government, as well as with ISACs (some of which have thousands of members) and ISAOs (which are largely in the development stage, with some notable exceptions).

- **Small Businesses and Underresourced Organizations: Indirect Beneficiaries of Innovations in Sharing.** Many small and midsize businesses, especially underresourced enterprises, will be able to benefit from an innovative, automated sharing ecosystem. A key long-term goal of information-sharing legislation is to foster economies of scale in real-time sharing. The Chamber anticipates that the marketplace will eventually provide inexpensive and simple-to-deploy technologies that conform to CISA's rules (e.g., scrubbing privacy information from CTIs) and generate and swap threat signatures at internet speeds. Systems like AIS will be able to block attacks sooner and more regularly, compared with the relatively human-intensive sharing schemes used today.

- **The Intrigued But Cautious: Sharing Should Pick Up as Both Education and Confidence Increase.** Businesses in this category have probably heard something about CISA through social media, cybersecurity events, and colleagues. Business leaders are interested in protected sharing arrangements, yet they are not ready to commit to routine sharing and receiving.

  Many cautious businesses have pictures in their heads of bureaucrats lying in wait with regulations and privacy groups readying lawsuits. The Chamber does not agree completely with these perspectives, but we hear them expressed frequently. Chamber staff attended a DHS-led C^3 Voluntary Program in early June in Indianapolis and one individual's remark comes to mind. He said, "I have heard about CISA. But we are not ready as a company to participate—it will take a cultural shift." This person's apprehension tells us how central it is that trust in CISA's protections be earned and maintained. The Chamber and most government leaders appreciate that business attitudes change over time and participation in CISA/AIS will be gradual.

  One change that may accelerate the use of CISA is business contracting arrangements. The Chamber foresees situations where large firms require their supply chain partners to belong to an ISAO/ISAC and to utilize AIS or some other automated means of timely indicator sharing.

- **ISAOs/ISACs Members: Leveraging the Expanding Network of Sharing Conduits.** Many members in this dispersed network of ISAOs/ISACs do not share cybersecurity threat data directly with the government. Instead, rank-and-file members in this category typically share CTIs and DMs with other businesses and with the government through the channels that information bodies (e.g., the Financial Services-ISAC, the Oil and Natural Gas-ISAC) provide. This category is expected to swell as confidence in the CISA program grows and new information-sharing organizations are stood up over the coming months and years. A Chamber member recently told us that she would engage CISA/AIS "gently and in steps—we'll build bit by bit." This mind-set is a useful window into how entities view the initiative.

The comparatively new ISAO standards organization is a key component of the Obama administration's cybersecurity strategy, launched in early 2015.[15] The administration's promotion of ISAOs is designed to encourage the protected sharing of information based on emerging and evolving threats that transcend industry sectors and geographic regions.[16] CISA is expected to have a positive influence on the expansion of the community of ISAOs and ISACs.

- **Early Information-Sharing Leaders: Increasing the Quality and Volume of Sharing Under CISA.** Private organizations in this category are actively engaged in sharing threat data. They were in the vanguard of businesses establishing and funding ISAOs and ISACs several years ago. Companies in this grouping have long-established information-sharing relationships among multiple industry peers and government partners, and several of them are already directly connected to sharing programs like AIS.[17]

  CISA should give lawyers and risk management professionals in these top organizations added certainty to receive cyber threat indicators (CTIs) and defensive measures (DMs) and to share them with business and government. A core purpose of the new law is to extend liability protections to companies to urge them to share cyber threat information.[18]

  Companies in this category are eager to see a sea change in the real-time sharing of threat indicators in and across sectors, as well as between government and businesses. According to a Chamber member who addressed the Commission on May 16, "Our adversaries should only use an attack or technique once. If our business spots an attack today, all businesses should be protected against it by day's end." Clearly, this company is an active member of the sharing community and wants public-private capacity to expand its capability to exchange threat data immediately. The Chamber agrees.

3. NORMS AND DETERRENCE: NEGOTIATING TOWARD ACCEPTABLE BEHAVIORS AND IMPOSING COSTS ON MALCIOUS ACTORS

Despite the existence of written blueprints, such as ones related to global prosperity and defense, the U.S. cybersecurity strategy is seemingly uncertain to many in the private sector and our adversaries alike. The Chamber believes that policymakers need to refocus national and global efforts to heighten the costs on sophisticated attackers that would willfully hack America's private sector for illicit purposes. Public-private policymaking needs to spotlight increasing adherence to international norms and deterrence, which is roughly equivalent to improving our defenses and imposing costs on bad actors, to reduce the benefits of conducting harmful cyber activity against the U.S. business community and the nation.

The Chamber believes that the Framework is a very useful tool in assisting businesses with strengthening their cybersecurity. However, much more needs to be done to give businesses and government the implements they need to adequately increase costs on malicious cyber activity. The Framework, intentionally or not, is a tactic in the United States' strategy to counter serious threats to our nation's economic and national security.

Over the past several years, policy and legislation have tended to focus almost exclusively on regulating industry (punishing the victim)[19] or leveraging trade and investment measures in economically risky ways, which the Chamber views as possibly a one-sided and losing proposition. Industry and government need to battle bad actors, not one another. Fortunately, due to NIST's work, the Framework should help create a more collaborative public-private approach to addressing cybersecurity threats, but the proof will be in the pudding.[20]

Our organization believes that the United States needs to coherently shift the costs associated with cyberattacks in ways that are timely, legal, and proportionate (relative to the risks and threats). Restraint needs to be the watchword, but nefarious actors that would attempt to empty bank accounts, steal trade secrets, or temporarily shut down vital infrastructure operations need to be held accountable. Policymakers need to help the law enforcement community. The FBI and the Secret Service are key assets to the business community.[21] But law enforcement officials are numerically overmatched compared with hackers. The Chamber supports increasing the resources that law enforcement agencies need to counter and mitigate cyber threats internationally.[22]

The Chamber believes that the next administration, Congress, and other stakeholders need to become more fluent concerning cyber deterrence, which is a new area of policy and practice. Participants need to conduct a review of actions that can be appropriately and wisely taken by business and government to deter bad actors. In a global security environment that is characterized by asymmetric threats and risks, businesses are frequently left to their own devices, which can give bad actors the upper hand, especially since offense in cyberspace is easy and defense is difficult.

The Chamber supports an open, innovative, and secure online environment that fosters commerce, not conflict. For norms and deterrence to be effective, businesses should have a menu of legal options at their disposal, sending a credible message that cyberattacks on industry and government will not be tolerated. After all, many policymakers and businesses are loath to tell illicit actors, "Do what you will—steal or damage our information—and we'll stand still." The realistic goal of improving deterrence policy and negotiating norms is to establish boundaries for what constitutes acceptable behavior in cyberspace for state and nonstate actors—the latter of which employ hit-and-run tactics online that are reminiscent of ocean-going piracy and age-old guerilla fighting.[23]

In early June, the Chamber's board approved a policy statement containing several recommendations concerning cybersecurity norms and deterrence, which our organization had been contemplating since 2013.[24] The full statement is provided for the Commission's review in the appendix to this letter.

The Chamber appreciates the opportunity to offer our views to the Commission regarding cybersecurity policy recommendations to the 45th presidency. We would be pleased to expand on the ideas in this letter. If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com; 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com; 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Appendix

U.S. Chamber of Commerce
Policy Statement on Cybersecurity Norms and Deterrence
June 2016

Three themes underpin the U.S. Chamber's policy statement on cybersecurity norms and deterrence, which focuses on principles (ideas that we believe in) and objectives (policies that we want pushed in collaboration with the U.S. government and foreign governments).

- The Chamber supports an open, innovative, and secure online environment that fosters commerce, not conflict.

- Cybersecurity improvement is inherently global in nature and requires norms or rules of the road that are effective across sectors and national boundaries.

- The United States and foreign governments need to make the private sector a genuine partner in crafting cyber policies, including policies related to defense, information sharing, privacy protections, and deterrence.

I. In consultation with the private sector and working with its allies and international organizations, the United States needs to continue developing its multiagency strategy for deterring and responding to cyber events through cyber and noncyber methods by employing all instruments of private and public power—diplomatic, economic, information, intelligence, military, and law enforcement. There is a problematic gap in current deterrence efforts between potential acts of cyberwar and low-level cyberattacks that bad actors are filling.

The Chamber generally agrees with the administration's 2015 policy regarding cyber deterrence. The administration prioritizes deterring cyberattacks[25] that threaten the loss of life and critical infrastructure systems and services, which would likely be equated as acts of war under international law. Top U.S. officials are rightly concerned about mitigating high-level threats that could cause "wide-scale disruption, destruction, loss of life, and significant economic consequences for the United States."[26]

But the cyber deterrence report is incomplete.[27] Businesses face an array of skilled and unskilled actors whose goals are to attack, disrupt, and exploit private networks and information systems. Such malicious incidents are occurring below the thresholds outlined in the deterrence policy, which only suggests if, when, and why the government may respond to incidents.

The Chamber believes that the administration's statement on deterrence, while taking many positive steps, does not adequately address the gap that exists between (1) major cyber incidents[28], which have not occurred yet, and (2) the more frequent, relatively minor attacks (e.g., pings) launched by unsophisticated actors that companies are capable of blunting mostly on their own and/or with the assistance of outside service providers.

Thus, in the malicious middle of the spectrum are costly[29] attacks against businesses that are linked to criminal groups and foreign powers or their surrogates that will virtually never be deterred, much less punished. National governments are either too slow, underresourced, or not well organized in cyberspace to respond fast and effectively. Costs—true calculus-changing costs that would alter the behavior of would-be attackers—are rarely imposed on bad actors.

The bottom line is that an improved deterrence policy, shaped by the United States and supported by its allies and other international partners, would better address the pernicious activities in the middle of the attack spectrum. The Chamber recognizes that this is not easy.[30]

II. Businesses' sound cyber risk management practices can make it harder for bad actors to succeed. Governments' cybersecurity policies and laws should be aligned with the approach underpinning the joint industry-National Institute of Standards and Technology's (NIST's) *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework).

Smart and effective cybersecurity practices can make it harder for bad actors to succeed against businesses, which some call "deterrence through denial." There is a broad consensus in U.S. industry that the Framework is an excellent baseline for businesses' cyber risk management programs and has the added benefit of being accessible to nontechnical professionals.[31]

The Framework is designed to help organizations start a cybersecurity program or improve an existing one. It puts cybersecurity into a common language for organizations to understand their cybersecurity posture, set goals for cybersecurity improvements, monitor their progress, and foster communications with internal and external stakeholders.

In addition to the Framework itself, the positive approach behind the Framework is just as significant. Use of the Framework is voluntary. Many industry and public-sector stakeholders are committed to a bottom-up, collaborative process to cybersecurity policy.[32] Also, a vigorous cybersecurity program—including against nation-state hackers or their surrogates and criminal syndicates—can be expensive. Therefore, it is imperative that the Framework processes remain cost effective. Organizations work mightily to get one dollar of security for every dollar spent.

Further, many Chamber members operate globally. We appreciate that NIST has been actively meeting with foreign governments urging them to embrace the framework. Like NIST, the Chamber believes that efforts to improve cybersecurity in the public and private sectors should reflect the borderless and interconnected nature of our digital environment.

The current administration and its successor should provide meaningful opportunities for private sector participation in multinational discussions. This could include creating dedicated public-private partnerships and other forums where multistakeholder experts provide input and best practices to ensure that any government activities reflect current technological developments. The Chamber urges the federal government to work with international partners and believes that these discussions should be stakeholder driven and occur routinely.

III. The United States and foreign governments should assist law enforcement entities in curtailing cybercrime. Authorities should also avoid blaming the victim, including placing disproportionate burdens for deterrence and liability on the private sector. Governments need to enhance their capacities to weaken nefarious organizations and individuals.

Cybercrimes are seemingly becoming more routine, more sophisticated, and more alarming. U.S. law enforcement is working diligently to bring domestic and foreign attackers to justice, which the Chamber applauds. The Chamber's cybersecurity campaign urges businesses to adopt fundamental internet security practices to reduce network and system weaknesses and make the price of successful hacking increasingly steep.

FBI and Secret Service agents participate at each of the Chamber's national cybersecurity events, and we urge businesses to report cyber incidents and online crime to government authorities. Our organization supports increasing the resources that law enforcement agencies need to counter and mitigate cyber threats, including investigating and prosecuting cybercrime cases internationally.[33]

As America's public and private sectors build on significant investments that they have made to strengthen the business community and U.S. economic security and resilience, other nations need to improve their capabilities. Fortunately, existing thinking points to some ways forward. For example, the Department of State's International Security Advisory Board (ISAB) issued draft recommendations in 2014 regarding cooperation and deterrence in cyberspace. The ISAB said that global cooperation against practices generally held as felonious, especially cybercrime and the theft of intellectual property (IP), should be a country's first step.

The Chamber holds that the U.S. government and its allies should build institutions in priority countries that foster a rule-of-law environment in ways that hit back at cybercrime and protects IP, consistent with the Budapest Convention on Cybercrime.[34] Indeed, the National Academies of Sciences noted, "When another nation's laws criminalize similar bad activities in cyberspace, the United States and other nation are more likely to be able to work together to combat hostile cyber operations that cross their national borders."[35]

The Chamber supports policies spotlighting foreign countries that need assistance with building capacity to battle cybercrime and enforce their laws against cyberattacks on American consumers and businesses. U.S. legislation could, for instance, enable the administration to identify countries of concern and fashion bilateral action plans to strengthen their legislative, institutional, and enforcement mechanisms.[36]

It is important to stress that companies hacked by foreign governments and amply resourced criminal groups often face unwarranted blame, including shouldering disproportionate burdens for deterrence and liability. Governments should reject a blame-the-victim mentality when it comes to cyber intrusions.[37]

IV. Countries need to dramatically reduce the theft of IP, including trade secrets.

IP-related industries generate 35% of America's economic output and are responsible for two-thirds of all exports and more than 40 million jobs. The threat of trade secrets theft is of increasing concern to U.S. economic well-being and job creation. The Chamber believes that Congress should pass legislation creating a federal civil cause of action to complement existing criminal remedies. A new legal structure would enable companies to better lessen the commercial injury and loss of employment that often occur when trade secrets are stolen, including via cyber methods.[38, 39]

Congress should increase resources for the Department of Justice (DOJ) and the FBI to investigate and prosecute cases of trade secrets theft.[40] Policymakers should support efforts by American private entities both to identify and recover or render inoperable IP stolen through cyber means.[41]

What's positive, Congress passed the Defend Trade Secrets Act of 2016 (P.L. 114–153) in April and the president signed it into law on May 11.

V. The United States and its allies should enhance businesses' situational awareness through protected information sharing.

The Chamber supported enactment of the Cybersecurity Information Sharing Act of 2015 (CISA), and we urge other democratic countries to adopt a public-private model for countering cyberattacks similar to CISA.[42] Some of the most virulent cyberattacks are originating from foreign states or their proxies and sophisticated criminals. CISA will help businesses better defend their networks and their customers' data.

CISA gives businesses legal certainty that they have protections against frivolous lawsuits when voluntarily sharing cyber threat information and taking actions to diminish cyberattacks. The legislation also offers safeguards related to public disclosure, regulatory, and antitrust matters. CISA reflects sound compromises among many stakeholders on these issues, and it promotes the goal of sharing threat data among multiple business and government entities while providing privacy protections.[43]

The Chamber believes that the information-sharing discussion puts insufficient emphasis on advancing government-to-business sharing. Federal agencies and departments need to push timely and actionable data to private entities, including businesses, information sharing and analysis centers (ISACs), and information sharing and analysis organizations (ISAOs). The government has gleaned threat data from hundreds of site visits and virtual engagements with public and private entities. Cybersecurity threat data would help the business community prioritize its risk mitigation activities.

VI. The United States and its trading partners must defend the freedom of international data flows.

Businesses, consumers, and governments all depend on and benefit from the seamless flow of data across borders. However, many governments increasingly cite privacy and security concerns to require data localization or create such high barriers to data transfers that de facto localization exists. The United States should push back against misguided arguments that data need to be stored or routed through domestic markets because such actions neither increase security nor enhance domestic economic growth. The United States should apply this same standard abroad and at home across all sectors.

Information security and privacy do not depend on the physical location of the data but, rather, on the protocols put in place wherever servers are located, as well as the processes followed whenever data are processed, transferred, and stored. Private organizations should be urged to implement cybersecurity risk management plans that offer the highest level of protection regardless of a server's location.

Businesses and consumers benefit when companies that maintain data are able to use cutting-edge security measures, regardless of the physical location of the data they seek to protect. Geographic neutrality with regard to data storage enables all companies, particularly small and midsize ones, to employ cost-effective information security solutions.

Relatedly, Mutual Legal Assistance Treaties (MLATs) must be implemented in a more efficient and transparent manner to remain effective for legitimate law enforcement needs. Governments are increasingly contacting companies directly to circumvent the slow process for gathering data outside a jurisdiction. However, this often results in companies facing a conflict of laws where they are put in the position of violating one law while trying to comply with another.

Businesses are encountering this dynamic in multiple parts of the world. Among the solutions needed is establishing a modernized approach that enables law enforcement to work with our allies to fight crime jointly by sharing evidence quickly and efficiently through clear rules. Improving the process for MLATs is a way to obviate the conflict of laws and streamline the process by which governments can access information related to bad actors outside their jurisdictions.

VII. States should seek international consensus on norms regarding conflict in cyberspace.

The U.S. government has identified approximately five peacetime norms of state behavior in cyberspace. In May 2015, Secretary of State John Kerry outlined key principles at Korea University, and they have subsequently been captured in the administration's cyber deterrence paper, excerpted below.[44, 45] The Chamber believes that these norms are a good start, and our organization's policy statement provides additional ideas for stakeholders to adopt.

1. A state should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public.

In March 2016, seven Iranians allegedly working on behalf of the Iranian government were indicted for a series of cybercrimes that cost U.S. financial institutions tens of millions of dollars and compromised critical controls of a New York dam, according to an FBI announcement. It is unclear if the indicted individuals will ever be brought to justice. However, the government's pursuit of cybercriminals through the use of all available tools, including public criminal charges, is valuable.[46]

2. A state should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents.

3. A state should not use CSIRTs to enable online activity intended to do harm.

4. A state should cooperate, in a manner consistent with its domestic law and international obligations, with requests for assistance from other states in investigating cybercrimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.

Norms are urgently needed when it comes to extraditing and prosecuting cybercriminals. There is no disincentive to being a cybercriminal that attacks U.S. industry from certain countries around the world. Recalcitrant governments too frequently will not help the U.S. government round up bad actors and turn them over to the FBI and the Secret Service.

5. A state should not conduct or *knowingly support* (or otherwise tolerate) cyber-enabled theft of IP within its jurisdiction, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors [italics added].[47]

The Chamber is concerned that the "knowingly support" wording is not sufficiently strong or clear. Such language could easily allow a country to ignore or deny activity emanating from its shores that is linked to IP theft.

On April 1, 2015, the White House issued an executive order (EO) intended to deter malicious cyber-enabled operations such as harming critical infrastructure, damaging computers, and stealing sensitive data. The new tool would allow the Department of the Treasury, in consultation with DOJ and the Department of State, to respond to cyber activities conducted from places beyond the reach of U.S. law enforcement.

Administration officials said that the authority would be used "judiciously" and in "extraordinary circumstances." However, officials expressed hope that other countries would adopt similar policies, creating the potential for governments to coordinate sanctions that reach across the globe.[48]

Sanctions are not a black or white issue. On the one hand, imposing economic costs through financial sanctions could offer an effective noncyber tool for responding to both cyberattacks and malicious cyber activities, including the theft of business trade secrets or the destruction of information devices and systems. On the other hand, the Chamber is generally opposed to sanctions because of the commercial harm and other negative effects that impact

trading partners. Tensions between countries could lead to retaliation from hostile nation-states against firms (e.g., the confiscation of a company's equipment and resources).

An open and constructive dialogue on challenging cybersecurity subjects like sanctions is crucial to improving cyber conflict management. Sanctions should be based on clear policy triggers (e.g., the 2015 EO on cyber sanctions),[49] be multilateral in nature, and constitute a government response of last resort. The U.S. government should consult closely with the business community before issuing penalties like sanctions so that authorities better understand the implications of policy actions.

The Chamber urges policymakers and members of the business community to become more familiar with concepts regarding international cybersecurity norms and deterrence. A growing body of writings affirms that existing international laws and norms apply to state behavior in cyberspace. In 2012, a Department of State official stressed, "Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint."[50] The challenge, though, is providing public- and private-sector decision makers with clear information to determine how global laws and norms apply to cyber activities.

The Chamber urges policymakers to clarify which authoritative resources and writings guide their thinking and deliberations. The 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare* is one such guide, as well as the June 2015 Department of Defense (DoD) *Law of War Manual*. Many terms—e.g., "cyberattack," which is often used colloquially to describe many types of hostile or malicious cyber activities; "computer network attack"; "use of force"; and "cyber espionage"—need further clarification. The list of cyber terminology is lengthy, sometimes confusing, and legalistic. Precise definitions are neither universally accepted nor understood.[51]

VIII. The U.S. government, like-minded nations, and businesses should oppose attempts to increase control of internet governance.

The Chamber believes that the multistakeholder bottom-up model of internet governance has proven successful and must be maintained in the future. Any attempts to increase government control of basic internet functions, such as domain names or standard protocols, must be prevented. This includes creating new government-controlled venues or trying to assert greater roles for existing government-controlled organizations, such as the United Nation's International Telecommunication Union (ITU).

IX. States should support public and private sector efforts that are under way to manage cyber supply chain risk.

The Chamber's cybersecurity education roundtable series urges businesses to use the NIST Framework when communicating with partners, vendors, and suppliers. Businesses of all sizes find it challenging to identify their risks and prioritize their actions to reduce weak links vulnerable to penetration, theft, and disruption. Our organization believes that NIST should provide additional guidance in this area, which the agency recognizes.

The Chamber's 2013 policy statement on information and communications technology (ICT), the supply chain, and government's regulatory role addresses managing cybersecurity supply chain risks, but we want to capture a few key points here:

- The Chamber supports efforts by policymakers to enhance the security of government ICT networks and systems, or the cyber supply chain. However, we urge policymakers to reject prescriptive and/or excessive supply chain or software assurance regimes that inject the United States or foreign governments directly into businesses' innovation and technology development processes, which are global in scope.

- Ambitious public- and private-sector efforts are under way to manage cyber supply chain risk. The Chamber opposes government actions that would create U.S.-specific guidelines, set private sector security standards, or conflict with industry-led security programs. Instead, the government should seek to leverage mutually recognized international agreements that enable ICT manufacturers to build products once and sell them globally.

- The Chamber has a fundamental concern about policies that would broadly apply restrictions on international commerce based on real or perceived threats to the cyber supply chain and ICT products' country of origin. ICT cybersecurity policy must be geared toward embracing globally recognized standards, facilitating trade, and managing risk.

X. States should help the private sector detect, contain, respond to, and recover from events in cyberspace. A new legal architecture—one that allows private organizations to assertively defend their networks and systems—needs to be considered by policymakers.

First, the administration needs to complete work on a national cybersecurity incident response plan (NCIRP), which has languished for several years. Certainly, a document alone would not beat back nation-state cyberattacks, cybercrime, cyber-enabled economic espionage, and other illicit activities. But an NCIRP would help formalize voluntary partnerships with government entities to counter potentially high consequence cyberattacks.[52]

Second, policymakers need to clarify the rights (e.g., self-defense), roles, and responsibilities of the public and private sectors. On paper, federal roles and responsibilities are fairly well delineated. The U.S. government assigns DOJ and the FBI with investigating and prosecuting cybercrimes. DHS is given the role of leading the protection of critical infrastructure. DoD is tasked with defending the nation from attack.

At the time of this writing in June, Presidential Policy Directive 41, *United States Cyber Incident Coordination*, had not been released.[53]

But most members of the business community are unclear when their obligations to guard their enterprises from a cyberattack ends, particularly in the face of a nation-state or a terrorist attack, and the government's responsibilities begins. The process for handing off the baton—

which, in reality, would highlight more, rather than less, public-private teamwork—warrants deeper discussion, comprehension, and exercise.

Third, the Chamber supports liability protections for businesses that use countermeasures to beat back malicious actors in cybersecurity. More broadly, businesses and private organizations should be allowed to assertively defend their data, devices, networks, and information systems within a legal framework. Indeed, passive behavior is not optimal for strong cyber defenses, and aggressive actions can be equally self-defeating.

Guidelines and legal protections are required to resolve the ambiguity that accompanies the private sector's efforts to defend its resources and capabilities in cyberspace. Such a forceful, yet disciplined, construct must be established by Congress with input from stakeholders.

The government has committed vast sums to working with the private sector to battle cyberattacks against the business community. Yet government entities are arguably hesitant to confront the vast majority of the cyber hostilities that beset the private sector. Businesses are affected daily across the globe by four dynamics, which explain the need for a new protective architecture.

- It is positive that businesses' cybersecurity budgets are increasing. Cyber defense is an ongoing challenge, especially as technology changes and adversaries adapt their tactics. However, the costs—e.g., legal, monetary, and reputational—of cyberattacks that hurt businesses are rising with little to no end in sight.

- Fundamental to any response to a cyberattack requires singling out the offender—attribution. The discussion related to attribution in cyberspace is evolving too slowly to support deterrence fully. A broader debate about the role of attribution in stopping or degrading malicious behavior could lead to improvements in organizations' cybersecurity. Attributing cyberattacks is part art, part science, and part politics. No series of technical and forensics actions by themselves can achieve a high degree of certainty about culpability. Individuals, teams, and groups' cultures contribute substantially to attributing cyberattacks with relative certainty.

  The more significant that a cyberattack is, the more resources and political capital a government will devote to uncovering an operation and the bad actors behind it. Some experts suggest, "Governments get to decide how to do attribution, and they get to decide when attribution is good enough for action." Such a statement is reasonable. However, the Chamber believes that the U.S. government needs to collaborate with the business community in both pinpointing suspects and calibrating timely, legal, and proportionate responses.[54]

- Many agencies and departments respond to the unceasing attacks by regulating industry, which is contrary to public-private collaboration and costly. Regulations are, in a word, frustrating, and they often lag well behind the innovations and depredations of cyberattackers. Government mandates are particularly troubling to companies that spend millions of dollars annually on enterprise safeguards and essentially underwrite a portion

of U.S. economic security. Cyberattacks arguably separate private organizations from state protection, and regulation is frequently perceived to be the opposite of state protection.

- Cyberattackers are almost never punished for their illicit actions, so there is no reason why the Chamber and other stakeholders should expect that their behavior will stop. New legal initiatives need to be considered in productive and transparent ways.

Thus, it is reasonable to the Chamber that businesses should seek greater legal authority to defend themselves as they spend an ever-increasing amount of resources on security. Meanwhile, bad actors, that largely operate overseas, evade U.S. authorities and are aided by foreign governments that either sponsor the cyberattacks or cast a blind eye to such activities.

NOTES

[1] Department of Commerce, National Institute of Standards and Technology (NIST) comment request, "Information on Current and Future States of Cybersecurity in the Digital Economy," *Federal Register*, pgs. 52827–52829 (August 10, 2016).

[2] Executive Order (EO) 13718, *Commission on Enhancing National Cybersecurity* (February 9, 2016).

[3] The Chamber supports piloting a CIDAR—shorthand for a cyber incident data and analysis repository. In May, we sent a letter to the Department of Homeland Security (DHS) saying that (1) data submitted to a CIDAR need to be made anonymous, (2) additional sharing protections will probably be needed, and (3) an experimental CIDAR could offer tangible upsides to public- and private-sector cybersecurity. Comprehensive information about cyber events could help insurers expand cyber coverage and identify cybersecurity best practices for their customers.

The idea behind the CIDAR is to provide a platform for enterprise owners and insurers to discreetly share, store, aggregate, and analyze sensitive cyber incident data. The CIDAR should specifically aid in expanding the "cyber" insurance market in healthy ways. The Chamber wants to help increase the sound buying of cybersecurity insurance beyond a few key sectors (e.g., banking and financial services, health care, retail, and technology) and large organizations, which are the principal purchasers of coverage today.

[4] The Chamber appreciates the efforts of the administration to renegotiate the Wassenaar Agreement (WA) control language governing so-called intrusion software and surveillance items, which are aspects of a controversial international agreement to prevent the export of sophisticated hacking tools to repressive governments and criminal organizations. Industry and democratic governments have a shared interest in keeping malicious software out of the hands of bad actors. But the 2013 WA control language governing intrusion software and surveillance items takes a seriously wrong approach to cybersecurity.

[5] Commission on Enhancing National Cybersecurity Commission (the Commission) Chair Thomas Donilon said in April, "The executive order also explicitly directs us to include other things that we think are important within this commission's work. We should also consider . . . making a stronger stance in the international realm going forward, with a *strong emphasis on deterrence* and developing international norms by working with countries who are willing to work on this topic" [italics added].

[6] See the Chamber-led March 11, 2016, group letter to the European Commission (EC). The EC requested stakeholders' views on cybersecurity public-private partnerships. The letter, signed by 19 industry associations, argues that embracing the Framework approach could advance the EU's goals for cybersecurity and a Digital Single Market (DSM).

[7] Information about the Commission on Enhancing National Cybersecurity's (the Commission's) meetings are available here.

[8] What particularly frustrates the Chamber about the Federal Communication Commission's (the FCC's or the Commission's) proposed rule is that we urge industry organizations to use the Framework and drive productive initiatives like public-private Communications Security, Reliability and Interoperability Council (CSRIC) IV's adoption in March 2015 of the *Cybersecurity Risk Management and Best Practices (Working Group 4)* report. However, the FCC is apparently backtracking on prior commitments to pursue a new regulatory model vis-à-vis the communications sector.

In June 2014, FCC leadership challenged the communications sector to "create a 'new regulatory paradigm' of business-driven cybersecurity risk management"—and sector stakeholders stepped up in a major way. The CSRIC IV endeavor both enhances the security of communications providers and protects individuals' privacy. But the Commission has seemingly turned its back on CSRIC IV in favor of "traditional regulation"—an approach that the FCC originally rejected.

It's worth noting that the Chamber wrote to the Cybersecurity Forum for Independent and Executive Branch Regulators (the Cyber Forum) on July 8. We argued that the interagency body should care a great deal about industry's views concerning the FCC's unwarranted regulatory actions. Government and businesses have mutual interests in fostering quality public-private cybersecurity relationships. Neither the Chamber nor the Cyber Forum should want to send industry the message that pursuing public-private partnerships comparable to CSRIC IV are hollow gestures.

The ink on the adaptive CSRIC IV initiative was barely dry before some authorities brushed it aside in favor of a compliance-based regime, which is ill-suited to respond effectively to today's complex cybersecurity environment. The Cyber Forum should understand that it's nearly impossible for the Chamber to promote public-private collaboration if only one party in the relationship is willing to make it work.

[9] The cyber legislation was included in the Consolidated Appropriations Act, 2016 (P.L. 114-113).

[10] See Automated Indicator Sharing (AIS) resources, including the Cybersecurity Information Sharing Act of 2015 (CISA) implementation procedures and guidance, available at www.us-cert.gov/ais. Also see pro-CISA advocacy papers: "It's About Protecting America's Cyber Networks, Not Surveilling You" (August 10, 2015); "Sharing Cyber Threat Indicators (CTIs)—Separating Fact From Fiction" (August 19, 2015); "'Voluntary' Means Voluntary—Separating Fact From Fiction" (August 26, 2015); and "Going on the 'Defensive'—Separating Fact From Fiction" (October 5, 2015). "Info-sharing debate shifts to implementation as privacy advocates now back cyber law," *Inside Cybersecurity* (June 13, 2016).

[11] DHS' Automated Indicator Sharing (AIS) capability.

[12] The AIS platform uses technical specifications, including the Trusted Automated eXchange of Indicator Information (TAXII), which defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information. It also uses Structured Threat Information eXpression (STIX), a collaborative effort to develop structured language to represent threat information. See "Homeland Security Department Launches Cyber Threat Sharing Platform," *The Wall Street Journal* (May 21, 2016).

[13] "CLTC-Hosted White House Commission Considers Challenges, Opportunities for the Next President" (June 27, 2016), University of California-Berkeley event summary.

[14] House Homeland Security Committee's Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee hearing, *Oversight of the Cybersecurity Act of 2015* (June 15, 2016).

[15] In February 2015, President Obama signed EO 13691 to promote cybersecurity information sharing among multiple business and government entities. The EO urges the private sector to develop information sharing and

analysis organizations (ISAOs) to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government.

[16] "ISAO standards body to issue next round of draft plans on info-sharing in July," *Inside Cybersecurity* (June 20, 2016).

[17] DHS' information sharing programs.

[18] "McCaul to evaluate effectiveness of cyber info-sharing law, including liability protections," *Inside Cybersecurity* (June 10, 2016).

[19] One speaker at the Commission's June 21 meeting in Berkeley, California, remarked, "Cyber is one of the few places where the victim is guilty and the attacker is the winner and gets all the reward. We've got to change that equation pretty quickly."

[20] On February 9, 2016, the Chamber sent a letter to the National Institute of Standards and Technology (NIST), commenting on the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework). Among the key points that our organization made in its letter are as follows:

- The Chamber has been actively promoting the Framework.
- Chamber members are using the Framework and urging business partners to manage cybersecurity risks to their information networks and systems.
- Our organization urges policymakers to help agencies and departments with streamlining existing regulations with the Framework and maintaining the Framework's voluntary nature.
- Industry opposes the creation of new or quasi-cybersecurity regulations, especially when government authorities have not taken affected entities' perspectives into account.

[21] See, for example, Matthew Weybrecht, "A DOJ Cybercrime Round Up", *Lawfare* blog (August 19, 2016).

[22] The table is meant to illustrate the numeric mismatch between government entities, including members of the Cyber Forum, that are empowered to regulate the business community and government entities that are tasked with investigating and prosecuting cybercrimes. The Cyber Forum should consider how its members can help law enforcement increase costs on malicious actors. We need more private sector and government capacity beyond the FBI and the Secret Service—which are just 2 federal entities out of 15 executive branch departments and dozens of independent agencies—pushing back on malicious actors. (See *The United States Government Manual, 2015*.)

Cybersecurity Forum for Independent and Executive Branch Regulators	
Members	Law enforcement role comparable to the FBI and the Secret Service? (Y/N)
Nuclear Regulatory Commission (NRC), chair	N
Federal Communications Commission (FCC)	N
Federal Energy Regulatory Commission (FERC)	N
Securities and Exchange Commission (SEC)	N
Federal Trade Commission (FTC)	N
Federal Reserve Board (Fed)	N
Federal Financial Institutions Examination Council (FFIEC)	N

Financial and Banking Information Infrastructure Committee (FBIIC)	N
National Association of Insurance Commissioners (NAIC)	N
Other agencies or departments may participate as appropriate	TBD
National Institute of Standards and Technology (NIST), a nonregulatory body, serves as an adviser to the Cyber Forum	NA

Policymakers need to help the law enforcement community, which is a key asset of the business community but numerically overmatched compared with hackers. The DOJ's John Carlin recently wrote an article in the *Harvard National Security Journal*, noting, "No one agency can beat the threat. Instead, success requires drawing upon each agency's unique expertise, resources, and legal authorities, and using whichever tool or combination of tools will be most effective in disrupting a particular threat." See "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats," *Harvard National Security Journal*, Volume 7, Issue 2 (June 20, 2016). Listen to "The Lawfare Podcast: John Carlin Uses All the Tools" (July 2, 2016).

[23] To guard the value of cyberspace and the internet, industry and U.S. policymakers need to focus on creating adaptive and decentralized tactics, techniques, and procedures (TTPs) that better help businesses and government entities respond swiftly to a messy cybersecurity environment. Simply put, it is probably not enough to confront cyberattacks as we want to but as we need to. To tweak a phrase that's well known among counterinsurgency advocates and critics, cybersecurity practitioners need to *learn how to eat soup with a mouse*. See, for example, John Nagl, *Knife Fights: A Memoir of Modern War in Theory and Practice* (New York: The Penguin Press, 2014.)

[24] See the section titled "Deterring bad actors: The need to clarify and strengthen U.S. cybersecurity strategy," (pg. 8) in the U.S. Chamber's December 13, 2013, letter to NIST concerning the preliminary Framework.

[25] According to the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Oxford, 2013), (pgs. 4, 48, and 106), a "cyberattack" refers to a cyber operation, "whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects," which are uses of force under international law. The Chamber understands that the U.S. government considers the *Tallinn Manual* largely an academic publication, which suggests that the document informs but does not determine U.S. policy.

[26] The administration's December 2015 cybersecurity deterrence report (deterrence report) to Congress, called for in section 941 of the fiscal year 2014 defense authorization bill (P.L. 113–66), prioritizes threats that the United States will seek to deter and includes the following:

- Cyberattacks or other malicious cyber activity intended to cause casualties.
- Cyberattacks or other malicious cyber activity intended to cause significant disruption to the normal functioning of U.S. society or government, including attacks against critical infrastructure that could damage systems used to provide key services to the public or the government.
- Cyberattacks or other malicious cyber activity that threatens the command and control of U.S. military forces, the freedom of maneuver of U.S. military forces, or the infrastructure on which the U.S. military relies to defend U.S. interests and commitments.
- Malicious cyber activity that undermines national economic security through cyber-enabled economic espionage or sabotage. Such activity undermines the fairness and transparency of global commerce as U.S. competitors steal developing technologies, win contracts unfairly, or steal information to manipulate markets and benefit their companies directly (pg. 3).

[27] Many key ideas concerning deterrence policy are described at length in Martin Libicki's book *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009).

[28] Michael Schmitt and Liis Vihul, Tallinn Paper No. 5: *The Nature of International Law Cyber Norms*, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2014).

[29] Most small and midsize businesses (SMBs), and even some large ones, lack the money and personnel to beat back advanced and persistent threats—popularly known as APTs in cybersecurity jargon—from breaching an organization's cyber defenses. Policymakers have not sufficiently acknowledged this expensive, practical reality. American companies should not be expected to shoulder the substantial costs of cyberattacks emanating from well-resourced bad actors such as criminal syndicates or nation-states—costs typically absorbed by national governments.

In 2015, Director of National Intelligence (DNI) James Clapper testified before Congress, saying, "Numerous actors remain undeterred from conducting economic cyber espionage or perpetrating cyberattacks. The absence of universally accepted and enforceable norms of behavior in cyberspace has contributed to this situation."

[30] The Obama administration says that its deterrence policy will adapt to new threats and geopolitical actions. The Chamber wants to work with the administration and its successor, as well as a range of stakeholders, to shrink this troublesome gap. It is a key area where additional work in the area of deterrence policy and international norms is especially needed.

[31] See endnote No. 3.

[32] Scott Shackelford, Scott Russell, and Jeffrey Haut, *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks* (December 10, 2015). UC Davis *Business Law Journal*, 2016; Kelley School of Business Research Paper No. 16–2.

[33] "Department of Justice FY 2017 Budget Request" (February 9, 2016); "Written testimony of USSS Director Joseph Clancy for a House Committee on Appropriations, Subcommittee on Homeland Security hearing on the Secret Services' Fiscal Year 2017 budget request" (March 15, 2016).

[34] *The IP Commission Report* (May 22, 2013), pg. 77.

[35] *Report on a Framework for International Cyber Stability*, International Security Advisory Board, U.S. Department of State (July 2, 2014).

[36] For example, the Chamber supported the International Cybercrime Reporting and Cooperation Act, legislation introduced in 2011 in the House and Senate.

[37] Assistant Attorney General for National Security John Carlin said, "Blaming companies for sophisticated breaches by nation-states is akin to blaming a pedestrian who gets stabbed by a stranger for simply making eye contact beforehand." See "DOJ official: Hacked companies face unwarranted blame," *Inside Cybersecurity* (May 27, 2015).

[38] See the Chamber's April 4, 2016, key vote letter to the Senate in support of S. 1890, the Defend Trade Secrets Act of 2016. The bill would provide companies with an effective tool to combat theft of trade secrets, a form of intellectual property (IP). By creating a federal civil remedy for trade secrets theft, this bill would help ensure that the trade secrets of U.S. companies are given similar protections afforded to other forms of IP, along with patents, trademarks, and copyrights.

[39] Defend Trade Secrets Act of 2016, Senate Judiciary Committee report (114–220, March 7, 2016), pg. 2.

[40] *The IP Commission Report*, pg. 67.

[41] Ibid, pg. 81.

[42] The Cybersecurity Information Sharing Act of 2015 (CISA) is title I of division N, the Cybersecurity Act of 2015, of the 2016 consolidated appropriations law (P.L. 114–113).

[43] See endnote No. 7.

[44] See the administration's deterrence report, pgs. 16–17, or Secretary of State John Kerry's remarks.

[45] The Department of State's March 2016 *International Cyberspace Policy Strategy*, called for under section 402 of the Cybersecurity Act of 2015, was transmitted to Congress in April. The Chamber obtained a copy of the strategy on May 9. The paper prioritizes many themes that are outlined in the Chamber's cyber norms and deterrence policy statement.

[46] FBI news release, "International Cyber Crime: Iranians Charged with Hacking U.S. Financial Sector," (March 24, 2016).

[47] The administration's deterrence report, pg. 17.

[48] "White House official: New cyber sanctions authority intended to be deterrent," *Inside Cybersecurity* (April 1, 2015).

[49] On December 31, 2015, the Department of the Treasury issued a final rule to implement President Obama's April 2015 executive order on cyber sanctions.

[50] Remarks by Harold Hongju Koh, Legal Advisor, U.S. Department of State, "International Law in Cyberspace" (September 18, 2012).

[51] See the Pentagon's *Law of War Manual* (June 2015), pgs. 994–2009.

[52] As noted in the February 9, 2016, White House announcement of the Cybersecurity National Action Plan (CNAP), the administration expects to "release a policy for national cyber incident coordination and an accompanying severity methodology for evaluating cyber incidents so that government agencies and the private sector can communicate effectively and provide an appropriate and consistent level of response."

[53] Presidential Policy Directive 41, *United States Cyber Incident Coordination (July 26, 2016).*

[54] Thomas Rid and Ben Buchanan paper, *Attributing Cyber Attacks* (December 23, 2014), *Journal of Strategic Studies*.